2019-MAR-20
FSL version 7.6.101

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

24669 - Cisco Webex Network Recording Player Arbitrary Code Execution Vulnerabilities (cisco-sa-20190123-webex-rce)

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2019-1637, CVE-2019-1638, CVE-2019-1639, CVE-2019-1640, CVE-2019-1641

Description

Remote code execution vulnerabilities are present in some versions of Cisco WebEx Network Recording Players.

Observation

Cisco WebEx Network Recording Players are used to play WebEx sessions in ARF or WRF formats.

Remote code execution vulnerabilities are present in some versions of Cisco WebEx Network Recording Players. The flaws lie in improper validation of advanced recording format (ARF) and webex recording format (WRF) files. Successful exploitation could allow an attacker to execute remote code on the target system.

24882 - Cisco Nexus 9000 Series Switches Standalone NX-OS Mode Tetration Analytics Agent Arbitrary Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1618

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to an incorrect permissions setting. Successful exploitation could allow an attacker to cause execute arbitrary code on the target system.

24753 - Google Chrome Multiple Vulnerabilities Prior To 72.0.3626.81

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause denial-of-service conditions and conduct more attacks on the targeted system.

24873 - Cisco Webex Meetings Desktop App Command Injection Vulnerability

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2019-1674

Description

A vulnerability is present in some versions of Cisco Webex Meetings Desktop App.

Observation

Cisco Webex Meetings Desktop App is used to access WebEx meetings.

A vulnerability is present in some versions of Cisco Webex Meetings Desktop App. The flaw is due to insufficient validation of user-supplied parameters. Successful exploitation could allow local attacker to gain elevated privileges and execute arbitrary commands on the target system.

24877 - Cisco NX-OS Software Netstack Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1599

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the network stack. Successful exploitation could allow a remote attacker to cause a denial of service condition.

24886 - Cisco NX-OS Software Unauthorized Filesystem Access Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1601

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to failure to impose strict file system permissions. Successful exploitation could allow a remote attacker to bypass security restrictions and gain read and write access to critical configuration file on the target system.

24887 - Cisco NX-OS Software Bash Shell Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-1596

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to incorrect permissions of a system executable. Successful exploitation could allow an authenticated, local attacker to escalate their privilege level to root.

131313 - Debian Linux 9.0 DSA-4408-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-6256, CVE-2019-7314, CVE-2019-9215

Description

The scan detected that the host is missing the following update:
DSA-4408-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2019/dsa-4408

Debian 9.0
all
libusageenvironment3_2016.11.28-1+deb9u2
liblivemedia57_2016.11.28-1+deb9u2
liblivemedia-dev_2016.11.28-1+deb9u2
livemedia-utils_2016.11.28-1+deb9u2
libgroupsock8_2016.11.28-1+deb9u2
libbasicusageenvironment1_2016.11.28-1+deb9u2

132498 - Oracle VM OVMSA-2019-0009 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-17807, CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-16862, CVE-2018-18559, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0009

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2019-March/000931.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-124.26.1.el6uek
kernel-uek-4.1.12-124.26.1.el6uek

147717 - SuSE SLES 11 SP4 SUSE-SU-2019:13979-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10741, CVE-2017-18360, CVE-2018-19407, CVE-2018-19824, CVE-2018-19985, CVE-2018-20169, CVE-2018-9568, CVE-2019-7222

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13979-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005194.html

SuSE SLES 11 SP4
i586
ocfs2-kmp-trace-1.6_3.0.101_108.87-0.28.7.1
kernel-xen-3.0.101-108.87.1
ocfs2-kmp-xen-1.6_3.0.101_108.87-0.28.7.1
kernel-trace-3.0.101-108.87.1
kernel-ec2-devel-3.0.101-108.87.1
kernel-ec2-base-3.0.101-108.87.1
kernel-source-3.0.101-108.87.1
kernel-pae-base-3.0.101-108.87.1
kernel-xen-devel-3.0.101-108.87.1
kernel-xen-base-3.0.101-108.87.1
kernel-trace-base-3.0.101-108.87.1
kernel-syms-3.0.101-108.87.1
kernel-default-3.0.101-108.87.1
kernel-default-devel-3.0.101-108.87.1
kernel-ec2-3.0.101-108.87.1
kernel-default-base-3.0.101-108.87.1
kernel-trace-devel-3.0.101-108.87.1
ocfs2-kmp-default-1.6_3.0.101_108.87-0.28.7.1
kernel-pae-devel-3.0.101-108.87.1
kernel-pae-3.0.101-108.87.1
ocfs2-kmp-pae-1.6_3.0.101_108.87-0.28.7.1

x86_64
ocfs2-kmp-trace-1.6_3.0.101_108.87-0.28.7.1
kernel-xen-3.0.101-108.87.1
ocfs2-kmp-xen-1.6_3.0.101_108.87-0.28.7.1
kernel-trace-3.0.101-108.87.1

kernel-ec2-devel-3.0.101-108.87.1
kernel-ec2-base-3.0.101-108.87.1
kernel-source-3.0.101-108.87.1
kernel-xen-devel-3.0.101-108.87.1
kernel-xen-base-3.0.101-108.87.1
kernel-trace-base-3.0.101-108.87.1
kernel-syms-3.0.101-108.87.1
ocfs2-kmp-rt_trace-1.6_3.0.101_rt130_69.42-0.28.7.1
kernel-default-3.0.101-108.87.1
kernel-default-devel-3.0.101-108.87.1
kernel-ec2-3.0.101-108.87.1
ocfs2-kmp-rt-1.6_3.0.101_rt130_69.42-0.28.7.1
kernel-default-base-3.0.101-108.87.1
kernel-trace-devel-3.0.101-108.87.1
ocfs2-kmp-default-1.6_3.0.101_108.87-0.28.7.1

147718 - SuSE Linux 15.0 openSUSE-SU-2019:0327-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-9843, CVE-2018-3058, CVE-2018-3060, CVE-2018-3063, CVE-2018-3064, CVE-2018-3066, CVE-2018-3143, CVE-2018-3156, CVE-2018-3162, CVE-2018-3173, CVE-2018-3174, CVE-2018-3185, CVE-2018-3200, CVE-2018-3251, CVE-2018-3277, CVE-2018-3282, CVE-2018-3284, CVE-2019-2510, CVE-2019-2537

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0327-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00057.html

SuSE Linux 15.0
i586
libmysqld19-debuginfo-10.2.22-lp150.2.9.1
mariadb-bench-debuginfo-10.2.22-lp150.2.9.1
libmysqld19-10.2.22-lp150.2.9.1
mariadb-debugsource-10.2.22-lp150.2.9.1
mariadb-test-debuginfo-10.2.22-lp150.2.9.1
mariadb-tools-10.2.22-lp150.2.9.1
mariadb-galera-10.2.22-lp150.2.9.1
mariadb-client-10.2.22-lp150.2.9.1
libmysqld-devel-10.2.22-lp150.2.9.1
mariadb-client-debuginfo-10.2.22-lp150.2.9.1
mariadb-test-10.2.22-lp150.2.9.1
mariadb-10.2.22-lp150.2.9.1
mariadb-debuginfo-10.2.22-lp150.2.9.1
mariadb-bench-10.2.22-lp150.2.9.1
mariadb-tools-debuginfo-10.2.22-lp150.2.9.1

noarch
mariadb-errormessages-10.2.22-lp150.2.9.1

x86_64
libmysqld19-debuginfo-10.2.22-lp150.2.9.1
mariadb-bench-debuginfo-10.2.22-lp150.2.9.1

libmysqld19-10.2.22-lp150.2.9.1
mariadb-debugsource-10.2.22-lp150.2.9.1
mariadb-test-debuginfo-10.2.22-lp150.2.9.1
mariadb-tools-10.2.22-lp150.2.9.1
mariadb-galera-10.2.22-lp150.2.9.1
mariadb-client-10.2.22-lp150.2.9.1
libmysqld-devel-10.2.22-lp150.2.9.1
mariadb-client-debuginfo-10.2.22-lp150.2.9.1
mariadb-test-10.2.22-lp150.2.9.1
mariadb-10.2.22-lp150.2.9.1
mariadb-debuginfo-10.2.22-lp150.2.9.1
mariadb-bench-10.2.22-lp150.2.9.1
mariadb-tools-debuginfo-10.2.22-lp150.2.9.1

147721 - SuSE Linux 15.0 openSUSE-SU-2019:0326-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12473, CVE-2018-12474, CVE-2018-12476

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0326-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00056.html

SuSE Linux 15.0
noarch
obs-service-obs_scm-common-0.10.5.1551309990.79898c7-lp150.2.3.1
obs-service-snapcraft-0.10.5.1551309990.79898c7-lp150.2.3.1
obs-service-appimage-0.10.5.1551309990.79898c7-lp150.2.3.1
obs-service-obs_scm-0.10.5.1551309990.79898c7-lp150.2.3.1
obs-service-tar-0.10.5.1551309990.79898c7-lp150.2.3.1
obs-service-tar_scm-0.10.5.1551309990.79898c7-lp150.2.3.1

147722 - SuSE Linux 15.0 openSUSE-SU-2019:0325-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-0886, CVE-2018-1000852, CVE-2018-8784, CVE-2018-8785, CVE-2018-8786, CVE-2018-8787, CVE-2018-8788, CVE-2018-8789

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0325-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00058.html

SuSE Linux 15.0
x86_64
freerdp-debugsource-2.0.0~rc4-lp150.2.3.1
freerdp-wayland-2.0.0~rc4-lp150.2.3.1
libfreerdp2-2.0.0~rc4-lp150.2.3.1
freerdp-debuginfo-2.0.0~rc4-lp150.2.3.1
freerdp-server-debuginfo-2.0.0~rc4-lp150.2.3.1
freerdp-wayland-debuginfo-2.0.0~rc4-lp150.2.3.1
libuwac0-0-debuginfo-2.0.0~rc4-lp150.2.3.1
libuwac0-0-2.0.0~rc4-lp150.2.3.1
uwac0-0-devel-2.0.0~rc4-lp150.2.3.1
freerdp-2.0.0~rc4-lp150.2.3.1
winpr2-devel-2.0.0~rc4-lp150.2.3.1
freerdp-devel-2.0.0~rc4-lp150.2.3.1
libwinpr2-2.0.0~rc4-lp150.2.3.1
freerdp-server-2.0.0~rc4-lp150.2.3.1
libfreerdp2-debuginfo-2.0.0~rc4-lp150.2.3.1
libwinpr2-debuginfo-2.0.0~rc4-lp150.2.3.1

147723 - SuSE SLES 11 SP4 SUSE-SU-2019:13982-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13982-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005203.html

SuSE SLES 11 SP4
i586
libssh2-1-1.4.3-17.3.1

x86_64
libssh2-1-1.4.3-17.3.1

147724 - SuSE Linux 42.3 openSUSE-SU-2019:0348-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12178, CVE-2018-12180, CVE-2018-3630

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0348-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00079.html

SuSE Linux 42.3
i586
ovmf-tools-2017+git1492060560.b6d11d7c46-16.1
ovmf-2017+git1492060560.b6d11d7c46-16.1

noarch
qemu-ovmf-ia32-2017+git1492060560.b6d11d7c46-16.1
qemu-ovmf-x86_64-2017+git1492060560.b6d11d7c46-16.1

x86_64
ovmf-tools-2017+git1492060560.b6d11d7c46-16.1
ovmf-2017+git1492060560.b6d11d7c46-16.1
qemu-ovmf-x86_64-debug-2017+git1492060560.b6d11d7c46-16.1

147725 - SuSE SLES 11 SP4 SUSE-SU-2019:13976-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-19636, CVE-2018-19638, CVE-2018-19639, CVE-2018-19640

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13976-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005187.html

SuSE SLES 11 SP4
noarch
supportutils-1.20-122.9.1

147726 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0642-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-10916

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0642-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005205.html

SuSE SLED 12 SP3
x86_64
lftp-debugsource-4.7.4-3.6.1

lftp-debuginfo-4.7.4-3.6.1
lftp-4.7.4-3.6.1

SuSE SLED 12 SP4
x86_64
lftp-debugsource-4.7.4-3.6.1
lftp-debuginfo-4.7.4-3.6.1
lftp-4.7.4-3.6.1

SuSE SLES 12 SP4
x86_64
lftp-debugsource-4.7.4-3.6.1
lftp-debuginfo-4.7.4-3.6.1
lftp-4.7.4-3.6.1

SuSE SLES 12 SP3
x86_64
lftp-debugsource-4.7.4-3.6.1
lftp-debuginfo-4.7.4-3.6.1
lftp-4.7.4-3.6.1

147727 - SuSE Linux 42.3 openSUSE-SU-2019:0343-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-5787, CVE-2019-5788, CVE-2019-5789, CVE-2019-5790, CVE-2019-5791, CVE-2019-5792, CVE-2019-5793, CVE-2019-5794, CVE-2019-5795, CVE-2019-5796, CVE-2019-5797, CVE-2019-5798, CVE-2019-5799, CVE-2019-5800, CVE-2019-5801, CVE-2019-5802, CVE-2019-5803, CVE-2019-5804

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0343-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00072.html

SuSE Linux 42.3
x86_64
chromium-debugsource-73.0.3683.75-205.1
chromium-73.0.3683.75-205.1
chromedriver-73.0.3683.75-205.1
chromium-debuginfo-73.0.3683.75-205.1
chromedriver-debuginfo-73.0.3683.75-205.1

160531 - CentOS 7 CESA-2019-0512 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-17972, CVE-2018-18445, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
CESA-2019-0512

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.centos.org/pipermail/centos-announce/2019-March/023218.html

CentOS 7
x86_64
kernel-debug-devel-3.10.0-957.10.1.el7
kernel-tools-libs-3.10.0-957.10.1.el7
perf-3.10.0-957.10.1.el7
kernel-devel-3.10.0-957.10.1.el7
kernel-3.10.0-957.10.1.el7
bpftool-3.10.0-957.10.1.el7
kernel-tools-libs-devel-3.10.0-957.10.1.el7
kernel-tools-3.10.0-957.10.1.el7
kernel-headers-3.10.0-957.10.1.el7
kernel-debug-3.10.0-957.10.1.el7
python-perf-3.10.0-957.10.1.el7

noarch
kernel-doc-3.10.0-957.10.1.el7
kernel-abi-whitelists-3.10.0-957.10.1.el7

163824 - Oracle Enterprise Linux ELSA-2019-0512 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-17972, CVE-2018-18445, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
ELSA-2019-0512

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008553.html

OEL7
x86_64
perf-3.10.0-957.10.1.el7
kernel-devel-3.10.0-957.10.1.el7
kernel-tools-libs-devel-3.10.0-957.10.1.el7
kernel-debug-devel-3.10.0-957.10.1.el7
kernel-doc-3.10.0-957.10.1.el7
kernel-tools-3.10.0-957.10.1.el7
kernel-debug-3.10.0-957.10.1.el7
kernel-abi-whitelists-3.10.0-957.10.1.el7
kernel-headers-3.10.0-957.10.1.el7
kernel-tools-libs-3.10.0-957.10.1.el7
python-perf-3.10.0-957.10.1.el7
kernel-3.10.0-957.10.1.el7
bpftool-3.10.0-957.10.1.el7

194883 - Fedora Linux 29 FEDORA-2019-3ecff65275 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-1002105

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3ecff65275

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

kubernetes-1.12.5-2.fc29

196269 - Red Hat Enterprise Linux RHSA-2019-0512 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-17972, CVE-2018-18445, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
RHSA-2019-0512

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00021.html

RHEL7D
x86_64
perf-3.10.0-957.10.1.el7
kernel-devel-3.10.0-957.10.1.el7
kernel-debug-debuginfo-3.10.0-957.10.1.el7
kernel-tools-libs-devel-3.10.0-957.10.1.el7
kernel-3.10.0-957.10.1.el7
kernel-debug-devel-3.10.0-957.10.1.el7
kernel-debuginfo-3.10.0-957.10.1.el7
kernel-tools-debuginfo-3.10.0-957.10.1.el7
kernel-tools-3.10.0-957.10.1.el7
kernel-debug-3.10.0-957.10.1.el7
perf-debuginfo-3.10.0-957.10.1.el7
kernel-headers-3.10.0-957.10.1.el7
kernel-tools-libs-3.10.0-957.10.1.el7
python-perf-3.10.0-957.10.1.el7
bpftool-3.10.0-957.10.1.el7
kernel-debuginfo-common-x86_64-3.10.0-957.10.1.el7
python-perf-debuginfo-3.10.0-957.10.1.el7

noarch

kernel-doc-3.10.0-957.10.1.el7
kernel-abi-whitelists-3.10.0-957.10.1.el7

RHEL7S
noarch
kernel-doc-3.10.0-957.10.1.el7
kernel-abi-whitelists-3.10.0-957.10.1.el7

x86_64
perf-3.10.0-957.10.1.el7
kernel-devel-3.10.0-957.10.1.el7
kernel-debug-debuginfo-3.10.0-957.10.1.el7
kernel-tools-libs-devel-3.10.0-957.10.1.el7
kernel-3.10.0-957.10.1.el7
kernel-debug-devel-3.10.0-957.10.1.el7
kernel-debuginfo-3.10.0-957.10.1.el7
kernel-tools-debuginfo-3.10.0-957.10.1.el7
kernel-tools-3.10.0-957.10.1.el7
kernel-debug-3.10.0-957.10.1.el7
perf-debuginfo-3.10.0-957.10.1.el7
kernel-headers-3.10.0-957.10.1.el7
kernel-tools-libs-3.10.0-957.10.1.el7
python-perf-3.10.0-957.10.1.el7
bpftool-3.10.0-957.10.1.el7
kernel-debuginfo-common-x86_64-3.10.0-957.10.1.el7
python-perf-debuginfo-3.10.0-957.10.1.el7

RHEL7WS
x86_64
perf-3.10.0-957.10.1.el7
kernel-devel-3.10.0-957.10.1.el7
kernel-debug-debuginfo-3.10.0-957.10.1.el7
kernel-tools-libs-devel-3.10.0-957.10.1.el7
kernel-3.10.0-957.10.1.el7
kernel-debug-devel-3.10.0-957.10.1.el7
kernel-debuginfo-3.10.0-957.10.1.el7
kernel-tools-debuginfo-3.10.0-957.10.1.el7
kernel-tools-3.10.0-957.10.1.el7
kernel-debug-3.10.0-957.10.1.el7
perf-debuginfo-3.10.0-957.10.1.el7
kernel-headers-3.10.0-957.10.1.el7
kernel-tools-libs-3.10.0-957.10.1.el7
python-perf-3.10.0-957.10.1.el7
bpftool-3.10.0-957.10.1.el7
kernel-debuginfo-common-x86_64-3.10.0-957.10.1.el7
python-perf-debuginfo-3.10.0-957.10.1.el7

noarch
kernel-doc-3.10.0-957.10.1.el7
kernel-abi-whitelists-3.10.0-957.10.1.el7

24653 - Cisco IOS Software TCP Denial Of Service Vulnerability (cisco-sa-20190109-tcp)

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-0282

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw lies in TCP socket code. Successful exploitation could allow an attacker to cause a denial of service condition in the target system.

24862 - Cisco Nexus 9000 Series Switches Standalone NX-OS Mode Fibre Channel over Ethernet NPV Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-1617

Description

A denial of service vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A denial of service vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to improper processing of FCoE packets when the fcoe-npv feature is uninstalled. Successful exploitation could allow an attacker to cause a denial of service condition on the target system.

147715 - SuSE Linux 15.0 openSUSE-SU-2019:0345-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-10360, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0345-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00076.html

SuSE Linux 15.0
i586
libmagic1-5.32-lp150.6.3.1
python2-magic-5.32-lp150.6.3.1
file-debugsource-5.32-lp150.6.3.1
python3-magic-5.32-lp150.6.3.1
file-devel-5.32-lp150.6.3.1
libmagic1-debuginfo-5.32-lp150.6.3.1
file-5.32-lp150.6.3.1
file-debuginfo-5.32-lp150.6.3.1

noarch
file-magic-5.32-lp150.6.3.1

x86_64

libmagic1-5.32-lp150.6.3.1
python2-magic-5.32-lp150.6.3.1
file-debugsource-5.32-lp150.6.3.1
python3-magic-5.32-lp150.6.3.1
file-devel-32bit-5.32-lp150.6.3.1
file-devel-5.32-lp150.6.3.1
libmagic1-debuginfo-5.32-lp150.6.3.1
libmagic1-32bit-5.32-lp150.6.3.1
libmagic1-32bit-debuginfo-5.32-lp150.6.3.1
file-5.32-lp150.6.3.1
file-debuginfo-5.32-lp150.6.3.1

186610 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3911-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-8904, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
USN-3911-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004805.html

Ubuntu 16.04

file_5.25-2ubuntu1.2
libmagic1_5.25-2ubuntu1.2

Ubuntu 18.10

libmagic1_5.34-2ubuntu0.1
file_5.34-2ubuntu0.1

Ubuntu 18.04

libmagic1_5.32-2ubuntu0.2
file_5.32-2ubuntu0.2

194886 - Fedora Linux 29 FEDORA-2019-bf531902c8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-7572, CVE-2019-7573, CVE-2019-7574, CVE-2019-7575, CVE-2019-7576, CVE-2019-7577, CVE-2019-7578, CVE-2019-7635, CVE-2019-7636, CVE-2019-7637, CVE-2019-7638

Description

The scan detected that the host is missing the following update:
FEDORA-2019-bf531902c8

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=1

Fedora Core 29

SDL-1.2.15-37.fc29

194888 - Fedora Linux 28 FEDORA-2019-216ba46b12 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-18267, CVE-2018-13988, CVE-2018-16646, CVE-2018-19058, CVE-2018-19059, CVE-2018-19060, CVE-2018-19149, CVE-2018-20662, CVE-2019-7310

Description

The scan detected that the host is missing the following update:
FEDORA-2019-216ba46b12

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 28

mingw-poppler-0.62.0-3.fc28

194889 - Fedora Linux 29 FEDORA-2019-7085420900 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-16646, CVE-2018-19058, CVE-2018-19059, CVE-2018-19060, CVE-2018-19149, CVE-2018-20481, CVE-2018-20551, CVE-2018-20650, CVE-2018-20662, CVE-2019-7310

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7085420900

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

mingw-poppler-0.67.0-4.fc29

24796 - Splunk Enterprise Cross Site Scripting Vulnerability (SP-CAAAQAF)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2019-5727

Description

A vulnerability is present in some versions of Splunk Enterprise.

Observation

Splunk Enterprise is a platform for real-time operational intelligence.

A vulnerability is present in some versions of Splunk Enterprise. The flaw is due to insufficient validation of user-supplied input. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

24801 - (JSA10899) Juniper Junos OS Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0063

Description

A denial of service vulnerability is present in some versions of Juniper Junos OS.

Observation

Juniper Junos OS is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos OS. The flaw lies in the IP next-hop index database. Successful exploitation could allow a remote attacker to cause a denial of service condition in the target system.

24814 - Wireshark Multiple Vulnerabilities Prior To 2.4.13

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2019-9208, CVE-2019-9209, CVE-2019-9214

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

24858 - Wireshark Multiple Vulnerabilities Prior To 2.6.7

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2019-9208, CVE-2019-9209, CVE-2019-9214

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

24859 - Joomla Additional Warning In The Global Configuration Textfilter Settings Vulnerability (20190203)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2019-7739

Description

A vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A vulnerability is present in some versions of Joomla! CMS. The flaw lies in global configuration textfilter settings. Successful exploitation could allow an attacker to bypass security restrictions and affect the integrity of the target system.

24876 - Delta Electronics Delta Industrial Automation PMSoft Information Disclosure Vulnerability (ICSA-18-270-04)

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2018-14824

Description

A vulnerability in some versions of Delta Electronics PMSoft could lead to information disclosure.

Observation

Delta Industrial Automation PMSoft is a software development tool used for motion controllers.

A vulnerability in some versions of Delta Electronics PMSoft could lead to information disclosure. The flaw is due to out-of-bounds read when processing project files. Successful exploitation by an attacker could lead to information disclosure on the target.

24883 - (JSA10896) Juniper Junos OS Telnetd Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0061

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in the Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in telnetd service. Successful exploitation could allow an attacker to cause high CPU usage and denial of service condition on the targeted system.

24885 - Cisco NX-OS Software Cisco Fabric Services Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-1616

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to insufficient validation of Cisco Fabric Services packets. Successful exploitation could allow a remote attacker to cause a denial of service condition.

24888 - Cisco NX-OS Software Image Signature Verification Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-1615

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in Signature Verification feature of Cisco NX-OS. Successful exploitation could allow an authenticated, local attacker to bypass security restrictions on the target system.

147720 - SuSE SLES 11 SP4 SUSE-SU-2019:13981-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-3816, CVE-2019-3833

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13981-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005200.html

SuSE SLES 11 SP4
i586
openwsman-client-2.2.3-0.16.8.1
libwsman1-2.2.3-0.16.8.1
openwsman-server-2.2.3-0.16.8.1

x86_64
openwsman-client-2.2.3-0.16.8.1
libwsman1-2.2.3-0.16.8.1

openwsman-server-2.2.3-0.16.8.1

160532 - CentOS 7 CESA-2019-0597 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-0816

Description

The scan detected that the host is missing the following update:
CESA-2019-0597

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.centos.org/pipermail/centos-announce/2019-March/023222.html

CentOS 7
x86_64
cloud-init-18.2-1.el7.centos.2

160534 - CentOS 7 CESA-2019-0482 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-3804

Description

The scan detected that the host is missing the following update:
CESA-2019-0482

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.centos.org/pipermail/centos-announce/2019-March/023221.html

CentOS 7
i686
cockpit-ws-173.2-1.el7.centos

noarch
cockpit-machines-ovirt-173.2-1.el7.centos
cockpit-system-173.2-1.el7.centos

x86_64
cockpit-doc-173.2-1.el7.centos
cockpit-bridge-173.2-1.el7.centos
cockpit-173.2-1.el7.centos
cockpit-ws-173.2-1.el7.centos

163825 - Oracle Enterprise Linux ELSA-2019-0597 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-0816

Description

The scan detected that the host is missing the following update:
ELSA-2019-0597

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008587.html

OEL7
x86_64
cloud-init-18.2-1.0.1.el7_6.2

178706 - Gentoo Linux GLSA-201903-12 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-12

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201903-12

Affected packages:
net-libs/webkit-gtk < 2.22.6

178707 - Gentoo Linux GLSA-201903-13 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-13

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201903-13

Affected packages:
net-dns/bind < 9.12.1_p2-r1

178708 - Gentoo Linux GLSA-201903-15 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-15

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201903-15

Affected packages:
net-misc/ntp < 4.2.8_p13

178709 - Gentoo Linux GLSA-201903-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-10

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201903-10

Affected packages:
dev-libs/openssl < 1.0.2r

178710 - Gentoo Linux GLSA-201903-14 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-14

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201903-14

Affected packages:
dev-java/oracle-jdk-bin < 1.8.0.202
dev-java/oracle-jre-bin < 1.8.0.202

178711 - Gentoo Linux GLSA-201903-11 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-11

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201903-11

Affected packages:
net-libs/xrootd < 4.8.3

178712 - Gentoo Linux GLSA-201903-09 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201903-09

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201903-09

Affected packages:
sys-libs/glibc < 2.26.0

194881 - Fedora Linux 28 FEDORA-2019-efa799fd16 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-19935

Description

The scan detected that the host is missing the following update:
FEDORA-2019-efa799fd16

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 28

php-7.2.16-1.fc28

194884 - Fedora Linux 29 FEDORA-2019-f187a4df7a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-19935

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f187a4df7a

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

php-7.2.16-1.fc29

196271 - Red Hat Enterprise Linux RHSA-2019-0597 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-0816

Description

The scan detected that the host is missing the following update:
RHSA-2019-0597

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00030.html

RHEL7S
x86_64
cloud-init-18.2-1.el7_6.2

196273 - Red Hat Enterprise Linux RHSA-2019-0482 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-3804

Description

The scan detected that the host is missing the following update:
RHSA-2019-0482

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00017.html

RHEL7D
x86_64
cockpit-debuginfo-173.2-1.el7
cockpit-ws-173.2-1.el7
cockpit-doc-173.2-1.el7
cockpit-173.2-1.el7
cockpit-bridge-173.2-1.el7

noarch
cockpit-system-173.2-1.el7
cockpit-machines-ovirt-173.2-1.el7

RHEL7S
noarch
cockpit-system-173.2-1.el7
cockpit-machines-ovirt-173.2-1.el7

x86_64
cockpit-debuginfo-173.2-1.el7
cockpit-ws-173.2-1.el7
cockpit-doc-173.2-1.el7
cockpit-173.2-1.el7
cockpit-bridge-173.2-1.el7

RHEL7WS
x86_64
cockpit-debuginfo-173.2-1.el7
cockpit-ws-173.2-1.el7
cockpit-doc-173.2-1.el7
cockpit-173.2-1.el7
cockpit-bridge-173.2-1.el7

noarch
cockpit-system-173.2-1.el7
cockpit-machines-ovirt-173.2-1.el7

131312 - Debian Linux 9.0 DSA-4409-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-9735

Description

The scan detected that the host is missing the following update:
DSA-4409-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2019/dsa-4409

Debian 9.0
all
neutron-plugin-openvswitch-agent_2:9.1.1-3+deb9u1
neutron-plugin-linuxbridge-agent_2:9.1.1-3+deb9u1
neutron-l3-agent_2:9.1.1-3+deb9u1
neutron-common_2:9.1.1-3+deb9u1
neutron-macvtap-agent_2:9.1.1-3+deb9u1
neutron-metadata-agent_2:9.1.1-3+deb9u1
python-neutron_2:9.1.1-3+deb9u1
neutron-linuxbridge-agent_2:9.1.1-3+deb9u1
neutron-plugin-nec-agent_2:9.1.1-3+deb9u1
neutron-sriov-agent_2:9.1.1-3+deb9u1
neutron-dhcp-agent_2:9.1.1-3+deb9u1
neutron-metering-agent_2:9.1.1-3+deb9u1
neutron-server_2:9.1.1-3+deb9u1
neutron-openvswitch-agent_2:9.1.1-3+deb9u1

147711 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0609-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2510, CVE-2019-2537

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0609-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005192.html

SuSE SLED 12 SP4
x86_64
mariadb-debugsource-10.2.22-3.14.1
mariadb-10.2.22-3.14.1
mariadb-debuginfo-10.2.22-3.14.1
mariadb-client-debuginfo-10.2.22-3.14.1
mariadb-client-10.2.22-3.14.1

noarch
mariadb-errormessages-10.2.22-3.14.1

SuSE SLES 12 SP4
noarch
mariadb-errormessages-10.2.22-3.14.1

x86_64
mariadb-10.2.22-3.14.1
mariadb-debuginfo-10.2.22-3.14.1
mariadb-client-10.2.22-3.14.1
mariadb-debugsource-10.2.22-3.14.1

mariadb-client-debuginfo-10.2.22-3.14.1
mariadb-tools-10.2.22-3.14.1
mariadb-tools-debuginfo-10.2.22-3.14.1

147712 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0604-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11212, CVE-2019-2422

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0604-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005190.html

SuSE SLES 12 SP3
x86_64
java-1_7_1-ibm-plugin-1.7.1_sr4.40-38.34.1
java-1_7_1-ibm-alsa-1.7.1_sr4.40-38.34.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.40-38.34.1
java-1_7_1-ibm-1.7.1_sr4.40-38.34.1

SuSE SLES 12 SP4
x86_64
java-1_7_1-ibm-plugin-1.7.1_sr4.40-38.34.1
java-1_7_1-ibm-alsa-1.7.1_sr4.40-38.34.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.40-38.34.1
java-1_7_1-ibm-1.7.1_sr4.40-38.34.1

147713 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0617-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11212, CVE-2018-1890, CVE-2019-2422, CVE-2019-2449

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0617-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005195.html

SuSE SLES 12 SP3
x86_64
java-1_8_0-ibm-alsa-1.8.0_sr5.30-30.46.1
java-1_8_0-ibm-1.8.0_sr5.30-30.46.1
java-1_8_0-ibm-plugin-1.8.0_sr5.30-30.46.1

SuSE SLES 12 SP4
x86_64
java-1_8_0-ibm-alsa-1.8.0_sr5.30-30.46.1
java-1_8_0-ibm-1.8.0_sr5.30-30.46.1
java-1_8_0-ibm-plugin-1.8.0_sr5.30-30.46.1

147714 - SuSE Linux 15.0 openSUSE-SU-2019:0346-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11212, CVE-2019-2422

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0346-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00077.html

SuSE Linux 15.0
i586
java-1_8_0-openjdk-devel-debuginfo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-debugsource-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-devel-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-headless-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-demo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-accessibility-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-src-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-debuginfo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.201-lp150.2.12.1

noarch
java-1_8_0-openjdk-javadoc-1.8.0.201-lp150.2.12.1

x86_64
java-1_8_0-openjdk-devel-debuginfo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-debugsource-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-devel-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-headless-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-demo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-accessibility-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-src-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-debuginfo-1.8.0.201-lp150.2.12.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.201-lp150.2.12.1

147716 - SuSE SLES 11 SP4 SUSE-SU-2019:13978-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11212, CVE-2019-2422

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13978-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005193.html

SuSE SLES 11 SP4
i586
java-1_7_1-ibm-alsa-1.7.1_sr4.40-26.36.1
java-1_7_1-ibm-plugin-1.7.1_sr4.40-26.36.1
java-1_7_1-ibm-1.7.1_sr4.40-26.36.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.40-26.36.1

x86_64
java-1_7_1-ibm-alsa-1.7.1_sr4.40-26.36.1
java-1_7_1-ibm-plugin-1.7.1_sr4.40-26.36.1
java-1_7_1-ibm-1.7.1_sr4.40-26.36.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.40-26.36.1

160530 - CentOS 7 CESA-2019-0485 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11784

Description

The scan detected that the host is missing the following update:
CESA-2019-0485

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.centos.org/pipermail/centos-announce/2019-March/023220.html

CentOS 7
noarch
tomcat-docs-webapp-7.0.76-9.el7_6
tomcat-jsvc-7.0.76-9.el7_6
tomcat-servlet-3.0-api-7.0.76-9.el7_6
tomcat-javadoc-7.0.76-9.el7_6
tomcat-webapps-7.0.76-9.el7_6
tomcat-lib-7.0.76-9.el7_6
tomcat-admin-webapps-7.0.76-9.el7_6
tomcat-el-2.2-api-7.0.76-9.el7_6
tomcat-jsp-2.2-api-7.0.76-9.el7_6
tomcat-7.0.76-9.el7_6

163823 - Oracle Enterprise Linux ELSA-2019-0485 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11784

Description

The scan detected that the host is missing the following update:
ELSA-2019-0485

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008573.html
http://oss.oracle.com/pipermail/el-errata/2019-March/008554.html

OEL7
x86_64
tomcat-docs-webapp-7.0.76-9.el7_6
tomcat-jsvc-7.0.76-9.el7_6
tomcat-servlet-3.0-api-7.0.76-9.el7_6
tomcat-javadoc-7.0.76-9.el7_6
tomcat-webapps-7.0.76-9.el7_6
tomcat-lib-7.0.76-9.el7_6
tomcat-admin-webapps-7.0.76-9.el7_6
tomcat-el-2.2-api-7.0.76-9.el7_6
tomcat-jsp-2.2-api-7.0.76-9.el7_6
tomcat-7.0.76-9.el7_6

186606 - Ubuntu Linux 14.04 USN-3910-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-18241, CVE-2018-1120, CVE-2018-19985, CVE-2018-7740, CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3910-2

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004804.html

Ubuntu 14.04

linux-image-4.4.0-143-powerpc64-smp_4.4.0-143.169~14.04.2
linux-image-powerpc64-emb-lts-xenial_4.4.0.143.125
linux-image-4.4.0-143-generic-lpae_4.4.0-143.169~14.04.2
linux-image-lowlatency-lts-xenial_4.4.0.143.125
linux-image-4.4.0-143-powerpc-smp_4.4.0-143.169~14.04.2
linux-image-powerpc64-smp-lts-xenial_4.4.0.143.125
linux-image-aws_4.4.0.1039.40
linux-image-4.4.0-1039-aws_4.4.0-1039.42
linux-image-generic-lpae-lts-xenial_4.4.0.143.125
linux-image-4.4.0-143-lowlatency_4.4.0-143.169~14.04.2
linux-image-4.4.0-143-powerpc64-emb_4.4.0-143.169~14.04.2
linux-image-powerpc-smp-lts-xenial_4.4.0.143.125

linux-image-4.4.0-143-powerpc-e500mc_4.4.0-143.169~14.04.2
linux-image-generic-lts-xenial_4.4.0.143.125
linux-image-powerpc-e500mc-lts-xenial_4.4.0.143.125
linux-image-virtual-lts-xenial_4.4.0.143.125
linux-image-4.4.0-143-generic_4.4.0-143.169~14.04.2

186607 - Ubuntu Linux 16.04 USN-3910-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-18241, CVE-2018-1120, CVE-2018-19985, CVE-2018-7740, CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3910-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004803.html

Ubuntu 16.04

linux-image-4.4.0-1077-aws_4.4.0-1077.87
linux-image-4.4.0-143-powerpc-smp_4.4.0-143.169
linux-image-powerpc-e500mc_4.4.0.143.151
linux-image-4.4.0-143-powerpc64-smp_4.4.0-143.169
linux-image-powerpc64-smp_4.4.0.143.151
linux-image-powerpc64-emb_4.4.0.143.151
linux-image-4.4.0-1104-raspi2_4.4.0-1104.112
linux-image-4.4.0-143-lowlatency_4.4.0-143.169
linux-image-lowlatency_4.4.0.143.151
linux-image-4.4.0-143-generic-lpae_4.4.0-143.169
linux-image-4.4.0-1041-kvm_4.4.0-1041.47
linux-image-generic-lpae_4.4.0.143.151
linux-image-generic_4.4.0.143.151
linux-image-raspi2_4.4.0.1104.104
linux-image-snapdragon_4.4.0.1108.100
linux-image-4.4.0-143-generic_4.4.0-143.169
linux-image-4.4.0-143-powerpc64-emb_4.4.0-143.169
linux-image-4.4.0-1108-snapdragon_4.4.0-1108.113
linux-image-kvm_4.4.0.1041.41
linux-image-aws_4.4.0.1077.80
linux-image-4.4.0-143-powerpc-e500mc_4.4.0-143.169
linux-image-virtual_4.4.0.143.151
linux-image-powerpc-smp_4.4.0.143.151

186608 - Ubuntu Linux 12.04 USN-3908-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6133

Description

The scan detected that the host is missing the following update:

USN-3908-2

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004801.html

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.166.156
linux-image-3.13.0-166-generic_3.13.0-166.216~precise1
linux-image-3.13.0-166-generic-lpae_3.13.0-166.216~precise1
linux-image-3.13.0-166-lowlatency_3.13.0-166.216~precise1
linux-image-generic-lts-trusty_3.13.0.166.156

194885 - Fedora Linux 29 FEDORA-2019-74a285d0ad Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-9210

Description

The scan detected that the host is missing the following update:
FEDORA-2019-74a285d0ad

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=1

Fedora Core 29

advancecomp-2.1-9.fc29

196270 - Red Hat Enterprise Linux RHSA-2019-0485 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11784

Description

The scan detected that the host is missing the following update:
RHSA-2019-0485

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00019.html

RHEL7D
noarch
tomcat-docs-webapp-7.0.76-9.el7_6

tomcat-jsvc-7.0.76-9.el7_6
tomcat-servlet-3.0-api-7.0.76-9.el7_6
tomcat-javadoc-7.0.76-9.el7_6
tomcat-webapps-7.0.76-9.el7_6
tomcat-lib-7.0.76-9.el7_6
tomcat-admin-webapps-7.0.76-9.el7_6
tomcat-el-2.2-api-7.0.76-9.el7_6
tomcat-jsp-2.2-api-7.0.76-9.el7_6
tomcat-7.0.76-9.el7_6

RHEL7S
noarch
tomcat-docs-webapp-7.0.76-9.el7_6
tomcat-webapps-7.0.76-9.el7_6
tomcat-servlet-3.0-api-7.0.76-9.el7_6
tomcat-javadoc-7.0.76-9.el7_6
tomcat-jsvc-7.0.76-9.el7_6
tomcat-el-2.2-api-7.0.76-9.el7_6
tomcat-admin-webapps-7.0.76-9.el7_6
tomcat-lib-7.0.76-9.el7_6
tomcat-jsp-2.2-api-7.0.76-9.el7_6
tomcat-7.0.76-9.el7_6

RHEL7WS
noarch
tomcat-docs-webapp-7.0.76-9.el7_6
tomcat-webapps-7.0.76-9.el7_6
tomcat-servlet-3.0-api-7.0.76-9.el7_6
tomcat-javadoc-7.0.76-9.el7_6
tomcat-jsvc-7.0.76-9.el7_6
tomcat-el-2.2-api-7.0.76-9.el7_6
tomcat-admin-webapps-7.0.76-9.el7_6
tomcat-lib-7.0.76-9.el7_6
tomcat-jsp-2.2-api-7.0.76-9.el7_6
tomcat-7.0.76-9.el7_6

89010 - Slackware Linux 14.2 SSA:2019-077-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863

Description

The scan detected that the host is missing the following update:
SSA:2019-077-01

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.378113

Slackware 14.2
x86_64
libssh2-1.8.1-x86_64-1

i586

libssh2-1.8.1-i586-1

182931 - FreeBSD RubyGems Multiple Vulnerabilities (27b12d04-4722-11e9-8b7c-b5e01141761f)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-8320, CVE-2019-8321, CVE-2019-8322, CVE-2019-8323, CVE-2019-8324, CVE-2019-8325

Description

The scan detected that the host is missing the following update:
RubyGems -- multiple vulnerabilities (27b12d04-4722-11e9-8b7c-b5e01141761f)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/27b12d04-4722-11e9-8b7c-b5e01141761f.html

Affected packages:
ruby23-gems < 3.0.2
ruby24-gems < 3.0.2
ruby25-gems < 3.0.2

182932 - FreeBSD PowerDNS Insufficient Validation In The HTTP Remote Backend (6001cfc6-9f0f-4fae-9b4f-9b8fae001425)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-3871

Description

The scan detected that the host is missing the following update:
PowerDNS -- Insufficient validation in the HTTP remote backend (6001cfc6-9f0f-4fae-9b4f-9b8fae001425)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/6001cfc6-9f0f-4fae-9b4f-9b8fae001425.html

Affected packages:
powerdns < 4.1.7

182933 - FreeBSD Jupyter notebook Cross-site Inclusion (XSSI) vulnerability (72a6e3be-483a-11e9-92d7-f1590402501e)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
Jupyter notebook -- cross-site inclusion (XSSI) vulnerability (72a6e3be-483a-11e9-92d7-f1590402501e)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/72a6e3be-483a-11e9-92d7-f1590402501e.html

Affected packages:
py27-notebook < 5.7.6
py35-notebook < 5.7.6
py36-notebook < 5.7.6
py37-notebook < 5.7.6

182934 - FreeBSD PuTTY Security Fixes In New Release (46e1ece5-48bd-11e9-9c40-080027ac955c)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
PuTTY -- security fixes in new release (46e1ece5-48bd-11e9-9c40-080027ac955c)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/46e1ece5-48bd-11e9-9c40-080027ac955c.html

Affected packages:
putty < 0.71
putty-gtk2 < 0.71
putty-nogtk < 0.71

182935 - FreeBSD Rails Action View Vulnerabilities (1396a74a-4997-11e9-b5f1-83edb3f89ba1)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-5418, CVE-2019-5419

Description

The scan detected that the host is missing the following update:
Rails -- Action View vulnerabilities (1396a74a-4997-11e9-b5f1-83edb3f89ba1)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/1396a74a-4997-11e9-b5f1-83edb3f89ba1.html

Affected packages:
rubygem-actionview4 < 4.2.11.1
rubygem-actionview50 < 5.0.7.2
rubygem-actionview5 < 5.1.6.2

182936 - FreeBSD mozilla Multiple Vulnerabilities (05da6b56-3e66-4306-9ea3-89fafe939726)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-9788, CVE-2019-9789, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9793, CVE-2019-9794, CVE-2019-9795, CVE-2019-9796, CVE-2019-9797, CVE-2019-9798, CVE-2019-9799, CVE-2019-9801, CVE-2019-9802, CVE-2019-9803, CVE-2019-9804, CVE-2019-9805, CVE-2019-9806, CVE-2019-9807, CVE-2019-9808, CVE-2019-9809

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (05da6b56-3e66-4306-9ea3-89fafe939726)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/05da6b56-3e66-4306-9ea3-89fafe939726.html

Affected packages:
firefox < 66.0_3,1
waterfox < 56.2.9
seamonkey < 2.49.5
linux-seamonkey < 2.49.5
firefox-esr < 60.6.0,1
linux-firefox < 60.6.0,2
libxul < 60.6.0
thunderbird < 60.6.0
linux-thunderbird < 60.6.0

186609 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3909-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-3840

Description

The scan detected that the host is missing the following update:
USN-3909-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004802.html

Ubuntu 16.04

libvirt0_1.3.1-1ubuntu10.25
libvirt-bin_1.3.1-1ubuntu10.25

Ubuntu 18.10

libvirt-daemon_4.6.0-2ubuntu3.4
libvirt-clients_4.6.0-2ubuntu3.4
libvirt0_4.6.0-2ubuntu3.4

Ubuntu 18.04

libvirt-clients_4.0.0-1ubuntu8.8
libvirt0_4.0.0-1ubuntu8.8
libvirt-daemon_4.0.0-1ubuntu8.8

194882 - Fedora Linux 28 FEDORA-2019-0a381a82de Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0a381a82de

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 28

firefox-65.0.2-1.fc28

194887 - Fedora Linux 29 FEDORA-2019-d39d6cbd8d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d39d6cbd8d

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=1

Fedora Core 29

thunderbird-60.5.3-1.fc29

147719 - SuSE Linux 15.0 openSUSE-SU-2019:0344-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-3811

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0344-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00075.html

SuSE Linux 15.0
x86_64
libsss_certmap0-debuginfo-1.16.1-lp150.2.9.1
libipa_hbac-devel-1.16.1-lp150.2.9.1
sssd-proxy-1.16.1-lp150.2.9.1
python3-sss-murmur-1.16.1-lp150.2.9.1
sssd-ad-debuginfo-1.16.1-lp150.2.9.1
sssd-tools-1.16.1-lp150.2.9.1
sssd-wbclient-debuginfo-1.16.1-lp150.2.9.1
sssd-proxy-debuginfo-1.16.1-lp150.2.9.1
libipa_hbac0-debuginfo-1.16.1-lp150.2.9.1
sssd-krb5-debuginfo-1.16.1-lp150.2.9.1
libnfsidmap-sss-debuginfo-1.16.1-lp150.2.9.1
sssd-32bit-1.16.1-lp150.2.9.1
sssd-debugsource-1.16.1-lp150.2.9.1
sssd-ad-1.16.1-lp150.2.9.1
sssd-wbclient-devel-1.16.1-lp150.2.9.1
adcli-debuginfo-0.8.2-lp150.4.1
adcli-doc-0.8.2-lp150.4.1
libsss_certmap-devel-1.16.1-lp150.2.9.1
libsss_simpleifp-devel-1.16.1-lp150.2.9.1
libsss_nss_idmap0-1.16.1-lp150.2.9.1
sssd-wbclient-1.16.1-lp150.2.9.1
libnfsidmap-sss-1.16.1-lp150.2.9.1
sssd-dbus-debuginfo-1.16.1-lp150.2.9.1
python3-sssd-config-1.16.1-lp150.2.9.1
sssd-winbind-idmap-debuginfo-1.16.1-lp150.2.9.1
python3-sss-murmur-debuginfo-1.16.1-lp150.2.9.1
sssd-winbind-idmap-1.16.1-lp150.2.9.1
python3-sss_nss_idmap-debuginfo-1.16.1-lp150.2.9.1
sssd-ipa-debuginfo-1.16.1-lp150.2.9.1
sssd-tools-debuginfo-1.16.1-lp150.2.9.1
libipa_hbac0-1.16.1-lp150.2.9.1
sssd-ipa-1.16.1-lp150.2.9.1
sssd-32bit-debuginfo-1.16.1-lp150.2.9.1
python3-sss_nss_idmap-1.16.1-lp150.2.9.1
libsss_nss_idmap0-debuginfo-1.16.1-lp150.2.9.1
adcli-0.8.2-lp150.4.1
python3-sssd-config-debuginfo-1.16.1-lp150.2.9.1
libsss_idmap0-debuginfo-1.16.1-lp150.2.9.1
libsss_certmap0-1.16.1-lp150.2.9.1
sssd-debuginfo-1.16.1-lp150.2.9.1
libsss_simpleifp0-1.16.1-lp150.2.9.1
sssd-ldap-1.16.1-lp150.2.9.1
libsss_idmap0-1.16.1-lp150.2.9.1
sssd-ldap-debuginfo-1.16.1-lp150.2.9.1
libsss_simpleifp0-debuginfo-1.16.1-lp150.2.9.1
sssd-krb5-common-1.16.1-lp150.2.9.1
libsss_nss_idmap-devel-1.16.1-lp150.2.9.1
adcli-debugsource-0.8.2-lp150.4.1
sssd-krb5-1.16.1-lp150.2.9.1
python3-ipa_hbac-debuginfo-1.16.1-lp150.2.9.1
sssd-krb5-common-debuginfo-1.16.1-lp150.2.9.1
sssd-dbus-1.16.1-lp150.2.9.1

sssd-1.16.1-lp150.2.9.1
libsss_idmap-devel-1.16.1-lp150.2.9.1
python3-ipa_hbac-1.16.1-lp150.2.9.1

i586
libsss_certmap0-debuginfo-1.16.1-lp150.2.9.1
libipa_hbac-devel-1.16.1-lp150.2.9.1
sssd-proxy-1.16.1-lp150.2.9.1
python3-sss-murmur-1.16.1-lp150.2.9.1
sssd-ad-debuginfo-1.16.1-lp150.2.9.1
sssd-tools-1.16.1-lp150.2.9.1
sssd-wbclient-debuginfo-1.16.1-lp150.2.9.1
sssd-proxy-debuginfo-1.16.1-lp150.2.9.1
libipa_hbac0-debuginfo-1.16.1-lp150.2.9.1
sssd-krb5-debuginfo-1.16.1-lp150.2.9.1
libnfsidmap-sss-debuginfo-1.16.1-lp150.2.9.1
sssd-debugsource-1.16.1-lp150.2.9.1
sssd-ad-1.16.1-lp150.2.9.1
sssd-wbclient-devel-1.16.1-lp150.2.9.1
adcli-debuginfo-0.8.2-lp150.4.1
adcli-doc-0.8.2-lp150.4.1
libsss_certmap-devel-1.16.1-lp150.2.9.1
libsss_simpleifp-devel-1.16.1-lp150.2.9.1
libsss_nss_idmap0-1.16.1-lp150.2.9.1
sssd-wbclient-1.16.1-lp150.2.9.1
libnfsidmap-sss-1.16.1-lp150.2.9.1
sssd-dbus-debuginfo-1.16.1-lp150.2.9.1
python3-sssd-config-1.16.1-lp150.2.9.1
sssd-winbind-idmap-debuginfo-1.16.1-lp150.2.9.1
python3-sss-murmur-debuginfo-1.16.1-lp150.2.9.1
sssd-winbind-idmap-1.16.1-lp150.2.9.1
python3-sss_nss_idmap-debuginfo-1.16.1-lp150.2.9.1
sssd-ipa-debuginfo-1.16.1-lp150.2.9.1
sssd-tools-debuginfo-1.16.1-lp150.2.9.1
libipa_hbac0-1.16.1-lp150.2.9.1
sssd-ipa-1.16.1-lp150.2.9.1
python3-sss_nss_idmap-1.16.1-lp150.2.9.1
libsss_nss_idmap0-debuginfo-1.16.1-lp150.2.9.1
adcli-0.8.2-lp150.4.1
python3-sssd-config-debuginfo-1.16.1-lp150.2.9.1
libsss_idmap0-debuginfo-1.16.1-lp150.2.9.1
libsss_certmap0-1.16.1-lp150.2.9.1
sssd-debuginfo-1.16.1-lp150.2.9.1
libsss_simpleifp0-1.16.1-lp150.2.9.1
sssd-ldap-1.16.1-lp150.2.9.1
libsss_idmap0-1.16.1-lp150.2.9.1
sssd-ldap-debuginfo-1.16.1-lp150.2.9.1
libsss_simpleifp0-debuginfo-1.16.1-lp150.2.9.1
sssd-krb5-common-1.16.1-lp150.2.9.1
libsss_nss_idmap-devel-1.16.1-lp150.2.9.1
adcli-debugsource-0.8.2-lp150.4.1
sssd-krb5-1.16.1-lp150.2.9.1
python3-ipa_hbac-debuginfo-1.16.1-lp150.2.9.1
sssd-krb5-common-debuginfo-1.16.1-lp150.2.9.1
sssd-dbus-1.16.1-lp150.2.9.1
sssd-1.16.1-lp150.2.9.1
libsss_idmap-devel-1.16.1-lp150.2.9.1
python3-ipa_hbac-1.16.1-lp150.2.9.1

160533 - CentOS 7 CESA-2019-0483 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Low

CVE: CVE-2018-5407

Description

The scan detected that the host is missing the following update:
CESA-2019-0483

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.centos.org/pipermail/centos-announce/2019-March/023219.html

CentOS 7
x86_64
openssl-1.0.2k-16.el7_6.1
openssl-static-1.0.2k-16.el7_6.1
openssl-devel-1.0.2k-16.el7_6.1
openssl-perl-1.0.2k-16.el7_6.1
openssl-libs-1.0.2k-16.el7_6.1

i686
openssl-static-1.0.2k-16.el7_6.1
openssl-devel-1.0.2k-16.el7_6.1
openssl-libs-1.0.2k-16.el7_6.1

163826 - Oracle Enterprise Linux ELSA-2019-0483 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2018-5407

Description

The scan detected that the host is missing the following update:
ELSA-2019-0483

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008531.html

OEL7
x86_64
openssl-perl-1.0.2k-16.0.1.el7_6.1
openssl-static-1.0.2k-16.0.1.el7_6.1
openssl-1.0.2k-16.0.1.el7_6.1
openssl-libs-1.0.2k-16.0.1.el7_6.1
openssl-devel-1.0.2k-16.0.1.el7_6.1

196272 - Red Hat Enterprise Linux RHSA-2019-0483 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-2018-5407

Description

The scan detected that the host is missing the following update:
RHSA-2019-0483

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00016.html

RHEL7D
x86_64
openssl-libs-1.0.2k-16.el7_6.1
openssl-devel-1.0.2k-16.el7_6.1
openssl-debuginfo-1.0.2k-16.el7_6.1
openssl-static-1.0.2k-16.el7_6.1
openssl-perl-1.0.2k-16.el7_6.1
openssl-1.0.2k-16.el7_6.1

RHEL7S
x86_64
openssl-libs-1.0.2k-16.el7_6.1
openssl-devel-1.0.2k-16.el7_6.1
openssl-debuginfo-1.0.2k-16.el7_6.1
openssl-static-1.0.2k-16.el7_6.1
openssl-perl-1.0.2k-16.el7_6.1
openssl-1.0.2k-16.el7_6.1

RHEL7WS
x86_64
openssl-libs-1.0.2k-16.el7_6.1
openssl-devel-1.0.2k-16.el7_6.1
openssl-debuginfo-1.0.2k-16.el7_6.1
openssl-static-1.0.2k-16.el7_6.1
openssl-perl-1.0.2k-16.el7_6.1
openssl-1.0.2k-16.el7_6.1

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

194841 - Fedora Linux 28 FEDORA-2019-f0add5eed0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-5704

Update Details

Risk is updated

24668 - (HT209449) Apple Safari Vulnerabilities Prior To 12.0.3

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6228, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

Update Details

Risk is updated

147685 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0511-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

Update Details

Risk is updated

182920 - FreeBSD webkit-gtk Multiple Vulnabilities (e3aacd6d-3d01-434c-9330-bc9efd40350f)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

Update Details

Risk is updated

186577 - Ubuntu Linux 18.04, 18.10 USN-3889-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6212, CVE-2019-6215

Update Details

Risk is updated

194798 - Fedora Linux 29 FEDORA-2019-d645f4337d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6212, CVE-2019-6215

Update Details

Risk is updated

194827 - Fedora Linux 28 FEDORA-2019-5c54d58073 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6212, CVE-2019-6215

Update Details

Risk is updated

24783 - (HT209520) Apple iOS Multiple Vulnerabilities Prior To 12.1.4

Category: Wireless Assessment -> NonIntrusive -> iOS
Risk Level: Medium
CVE: CVE-2019-6223, CVE-2019-7286, CVE-2019-7287, CVE-2019-7288

Update Details
Risk is updated

194876 - Fedora Linux 29 FEDORA-2019-9a6906a128 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-17937

Update Details
Risk is updated

194880 - Fedora Linux 28 FEDORA-2019-3ee66c2020 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-17937

Update Details
Risk is updated

131303 - Debian Linux 9.0 DSA-4397-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2019-3824

Update Details
Risk is updated

182898 - FreeBSD botan2 Side Channel During ECC Key Generation (d8e7e854-17fa-11e9-bef6-6805ca2fa271)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-20187

Update Details
Risk is updated

186588 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3895-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium

CVE: CVE-2019-3824

Update Details

Risk is updated

194818 - Fedora Linux 29 FEDORA-2019-e0f5a82082 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-20187

Update Details

Risk is updated

70017 - cisco.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.